REMARKS

Applicants respectfully request reconsideration of the present application based on the foregoing amendments and following remarks. By this Amendment, claims 1, 2, 9, 12, 14, 15, 22, 25, 27 and 28 have been amended. Upon entry of this Amendment, claims 1-28 will remain pending in the application.

Claim Rejections Under 35 U.S.C. 112 (First Paragraph)

Claims 1-28 stand rejected under 35 U.S.C. 112 (first paragraph) for allegedly failing to comply with the written description requirement. Although Applicants respectfully disagree with the basis for this rejection, the claims have been amended in a manner which should obviate this rejection.

For example, the Office Action objected to the claim limitation "wherein the private key is not provided to the user" that was added by the previous amendment into each of the independent claims. Accordingly, this limitation has been removed. Instead each of the independent claims has been amended to require that the user's private key is stored at the authentication server, and the authentication server provides access for use in encrypting a request only if the user supplies a biometric sample that matches a biometric template. This subject matter is described in detail in the specification, for example at page 10, lines 1-3 and 5-9 : "However, **unlike conventional PKI's**, the user's private key 204 **is kept secret from the user and is stored on a secure server** and only accessed after a valid biometric signature has been authenticated." Moreover, the summary of the invention specifically explains how, in contrast to prior art PKI infrastructures, private keys are stored on a server that only allows them to be used for a transaction if the user supplies a successful biometric signature. For example, the summary states that "**this approach allows those private key(s) to be stored on a secure server that is accessed only after a biometric signature has been validated** (for example a fingerprint)." (page 6 lines 14-15, emphasis added). Still further, the present specification teaches that "In accordance with an aspect of the invention, authentication is based upon requiring biometric signature(s) to be matched against known templates in order to access **private keys stored on a secure server** before continuing transaction processing. BioPKI protects an individual's biometric characterization so that it cannot be compromised or abused.

This secured information is then used to retrieve a uniquely assigned **private key that can only be accessed via a biometric signature** to sign a transaction message context." (page 8, line 22 to page 9, line 7, emphasis added). Accordingly, the amended claims are fully supported by the specification as originally filed, and so the rejection should be withdrawn.

The Office Action also objected to claim 27, which was amended to specify that "the server encrypts the request with a private key." Although the basis for this objection is respectfully disagreed with, claim 27 has been amended to clarify that the server allows access to the private key for use in encrypting the user's request. This is supported by the specification as shown above, and so this objection should be overcome.

Finally, the Office Action also objected to claims 2 and 15 that specifies generating a digital signature using the private key and sending the digital signature to the user. Although Applicants respectfully disagree with the objection, the claims have been broadened so as not require that the digital signature is sent to the user, which should obviate the objection.

For at least the foregoing reasons, the 112 rejection of the claims should be withdrawn.

Claim Rejections Under 35 U.S.C. 102

Claims 1-5, 9-18 and 22-28 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,920,561 to Gould et al. ("Gould"). For reasons set forth more fully below, this rejection is respectfully traversed.

Amended Independent Claims 1, 14 and 27 Patentably Define Over Gould

Amended independent claims 1, 14 and 27 have been amended to clarify that the user's private key is stored at an authentication server and "access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template."

As set forth in previous responses, Gould merely teaches a "free seating" system where a user can use any client computer in a network to access the network. (Title) The client computers include a biometric scanning device to obtain samples from the user. (col. 5, lines 14-17) Each client computer already has and stores its own unique private key. (col. 5, lines 19-21).

After obtaining the user's sample and before the user is verified the client encrypts the sample with the client computer's private key and sends the encrypted sample to the server. (col. 5, lines 22-23). Clearly, Gould's system does **not** "[prevent] access to the private key stored at the authentication server for use in encrypting the user's request . . . unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template," as specifically required by the independent claims. Moreover, the private key for use in encrypting requests is not stored at the server in Gould's system, but in each client computer.

For at least these reasons, amended independent claims 1, 14 and 27 patentably define over Gould. Accordingly, the 102 rejection of claims 1, 14 and 27, together with claims 2-5 and 9-13 that depend from claim 1, claims 15-18 and 22-26 that depend from claim 14, and claim 28 that depends from claim 27, should be withdrawn.

The Dependent Claims Further Patentably Define Over Gould

All of the remaining rejected claims depend from independent claims 1, 14 and 27 and are patentable for at least the reasons presented above. Nevertheless, the dependent claims recite subject matter that still further patentably define over Gould.

Claims 3 and 16 require providing the digital signature that is generated per claims 2 and 15 to the service associated with the request. Gould's signature generated in step 416 is just provided back to the client, not to a service that the user is requesting. The Office Action points to Gould's client computer as both a client and a requested service per the claims. Applicants respectfully submit that this position does not afford each term in the claim its proper patentable weight (i.e. it is not considered necessary for the claims to be amended to require that the client and requested service are different things, because they should already be presumed to be different). The Office Action must specify whether Gould's client computer is the claimed client or the requested service. The Office Action cannot use the same element in a reference to meet two different and distinct claim elements.

If Gould's client computer and client are considered two different things, then Gould does not meet the claimed limitations. If they are considered to be two different things, then the computer itself (i.e. the alleged requested service) does not receive the signature generated in

step 416 (it is instead received by the separate and distinct client). Accordingly, either the Office Action's position is improper and/or Gould does not meet the explicit limitations of claims 3 and 16.

Claims 4 and 17 require providing a biometric signature corresponding to the biometric sample to the service associated with the request. Gould's signature generated in step 416 is just provided back to the client, not to a service that the user is requesting. As set forth above, the Office Action is not permitted to rely on one element in the prior art as meeting two distinct and different claim elements. Accordingly, Gould does not meet the explicit limitations of claims 4 and 17.

Claims 9 and 22 require including integrity information in an encrypted biometric sample that is collected for transmission to an authentication server. The Office Action merely points to a signature sent with an encrypted sample. There is no information included in the encrypted sample, much less integrity information as required by the claims. Accordingly, Gould does not meet the explicit limitations of claims 9 and 22.

Claims 10 and 23 require decrypting and checking the integrity information that is included and encrypted in claims 9 and 22. Gould's server 100 merely checks signature information that is sent with a collected sample, not integrity information in the encrypted sample. Accordingly, Gould does not meet the explicit limitations of claims 10 and 23.

Claims 11 and 24 require that the integrity information of claims 9 and 22 includes a unique transaction identifier. The Office Action once again only relies on the separate signature sent with the encrypted sample as the identifier, which is not in the encrypted sample. Accordingly, Gould does not meet the explicit limitations of claims 11 and 24.

Claims 12 and 25 require associating user identification information with the private key that is provided for use in encrypting the user's request depending on the biometric sample match. Claims 12 and 25 further require maintaining a certificate containing the user identification information. The Office Action points to Gould's database of user's biometric templates and user credentials that are sent to the client computer, and signed with a server private key. This is clearly not the same private key that is used to encrypt the user's request as required by the claims. Accordingly, Gould does not meet the explicit limitations of claims 12 and 25.

For at least these additional reasons, the dependent claims further patentably define over Gould and the rejections thereof should be withdrawn.

Claim Rejections Under 35 U.S.C. 103

Claims 6-8 and 19-21 stand rejected under 35 U.S.C. 103(a) as being obvious over Gould. For reasons set forth more fully below, this rejection is respectfully traversed.

Claims 6-8 depend from claim 1, and claims 19-21 depend from claim 14. Claims 1 and 14 have been shown above to be patentable over Gould because at least two elements required by the claims are completely missing from Gould. Accordingly, there is no prima facie case of obviousness against claims 1 and 14 either, and so the subject matter of claims 6-8 and 19-21 is not obvious in view of Gould for at least this reason.[1]

Moreover, Applicants respectfully disagree with the bases supplied in the Office Action for these rejections.

Specifically, the Office Action admits that Gould merely teaches creating a biometric template for a user. So the Office Action relies on Official Notice for the entire contents of six claims based on a mere familiarity with store credit cards. For example, claims 6-8 require: (a) generating pre-enrollment keys for the user; (b) supplying the pre-enrollment keys to respective key generators; (c) generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators; (d) verifying registration of the user in accordance with a comparison of the final enrollment key; (e) creating the biometric template for the user only if registration is verified; (f) generating the private key only if the biometric template is successfully created; and (g) associating user identification information with the final enrollment key.

The Office Action does not and cannot explain what credit card company creates a biometric template only if a registration is verified? What are the credit card "pre-enrollment" keys? What are the credit cad "final enrollment keys"? Who is the credit card "key

---

[1] The Office Action suggests that since this is a 103 rejection and not 102, that it is not necessary that the prior art show all claim limitations. This is wrong. MPEP 2143.03.

administrator"? Who are the credit card "key generators"? What credit card company only generates a private key if the biometric template is successfully created?

Applicants respectfully submit that the Office Action has reduced the invention to a "gist" of using two different persons to "enroll" a user, and considers this "gist" to be obvious. In so doing, the Office Action completely glosses over numerous explicit claim limitations. This is improper use of Official Notice and an improper basis of rejection under Rule 103.

For at least these additional reasons, the 103 rejection of claims 6-8 and 19-21 should be withdrawn.

Double Patenting

Claims 1, 13, 14, 26 and 27 stand provisionally rejected on the ground of nonstatutory obviousness-type double patenting in view of claims 1, 17, 18, 20, 36, 39 and 44 of co-pending application 09/801,468 ("the 468 Application"). For reasons set forth more fully below, this rejection is respectfully traversed.

The below table compare independent claims 1 and 27 in the present application, along with corresponding independent claims 1 and 39 from the '468 Application (claim 13 depends from claim 1, and claim 14 contains similar limitations as claim 1).[2] As indicated in bold in the table below, there are many elements in the present claims that are completely missing in the '468 Application claims, and vice-versa.

Present Application	'468 Application
1. A method comprising:	1. A method for **reducing the occurrence of unauthorized use of on-line resources**, comprising:
storing a private key associated with a user at an authentication server;	**storing business rules for a plurality of companies having on-line resources;**
receiving a request for access to a service from the user;	receiving a message indicating a request from a user to use on-line resources;

[2] The '468 Application claims have been amended and that application is currently on Appeal. The language above is from the '468 Application claims on Appeal. However, it is believed that the claims as originally filed in the '468 Application were also sufficiently distinctive to eliminate the basis for the rejection.

Present Application	'468 Application
	identifying a company associated with the requested on-line resource from among the plurality of companies;
	retrieving the stored business rules for the identified company;
	determining whether the request requires authentication;
	enabling the request to be fulfilled without authentication if the determination indicates that authentication is not required;
collecting a biometric sample from the user **via a client associated with the user and remote from the authentication server on a network;**	obtaining an indicia of physical identification from the user **if the determination instead indicates that authentication is required**;
sending the collected biometric sample from the client to the authentication server;	
comparing, **at the authentication server,** the biometric sample to a biometric template associated with the user; and	comparing the obtained indicia to a stored indicia for the user; and
if a result of the comparing step indicates a match between the biometric sample and template for the user:	**enabling the request to be fulfilled if the obtained indicia matches the stored indicia,**
allowing the private key from the authentication server to be accessed and used with the request;	**wherein the step of determining whether the request requires authentication includes determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.**
encrypting the request with a the private key, and	
providing the service with access to a public key corresponding to the private key,	
wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client	

Present Application	'468 Application
matches the biometric template.	
27. An authentication infrastructure comprising: a server that intercepts a request by a user for access to a service and **controls access to a stored private key associated with the user**; and **a client that collects a biometric sample from the user in response to the user making the request and sends the collected biometric sample to the server,** **wherein the server maintains a biometric template associated with the user for authenticating the collected biometric sample, and** **wherein, if and only if** the collected biometric sample matches the biometric template: **the server allows access to the stored private key for use in encrypting the request, so that the user need not maintain a token for accessing the service, and the user need not store the private key, and** **the server provides the service with access to a public key corresponding to the private key,** **wherein access to the private key stored at the server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric**	39. An apparatus **for reducing the occurrence of unauthorized use of on-line resources**, comprising: a server that is **adapted to communicate with a network based service** so as to receive a message indicating a request from a user to use the network based service; **a rules subsystem coupled to the server that determines whether the request requires authentication, the rules subsystem causing the server to enable the request to be fulfilled without authentication if the determination indicates that authentication is not required and causes the server to obtain an indicia of physical identification from the user if the rules subsystem instead determines that authentication is required; and** **a business rules database coupled to the rules subsystem, the database storing business rules for a plurality of companies having on-line resources;** an authentication subsystem coupled to the server that compares the obtained indicia to a stored indicia for the user, **wherein the rules subsystem is adapted to identify a company associated with the requested on-line resource from among the plurality of companies, retrieve the stored business rules for the identified company from the business rules database and determine whether the stored business rules for the identified company associated with the requested on-line resource requires authentication for the user, and** **wherein the server sends a signal to the network based service that the request is to be fulfilled if the authentication subsystem determines that the obtained indicia matches the stored indicia.**

Present Application	'468 Application
template.	

As can be clearly seen, there are multiple elements that are not included in the claims of the two commonly-owned applications, and so there is no prima facie support for the proposition that they are obvious in view of each other based on only the teachings of the claims themselves. Accordingly, the double patenting rejection should be withdrawn.

Conclusion

All objections and rejections having been addressed, the application is believed to be in condition for allowance and Notice to that effect is earnestly solicited. If any issues remain which the Examiner feels may be resolved through a telephone interview, s/he is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: April 26, 2007

40,580
Mark J. Danielson Reg. No.
(650) 233-4777
Please reply to customer no. 27,498